Attachment B: Factual Basis

Starting in at least December 2017, Shaimone Barkhadle engaged in a scheme to defraud real individuals, businesses, and banks out of money. He accomplished the scheme by, among other things, opening bank accounts and obtaining credit cards and a loan using the identity of a real individual, R.R., as well as opening accounts using the identity of fictitious individuals and businesses. Barkhadle then provided information on the accounts he fraudulently opened to coconspirators who funneled money from business email compromise frauds into those accounts. Once the fraudulently obtained funds entered Barkhadle's fraudulent accounts, Barkhadle moved the money to different fraudulent accounts and ultimately withdrew the funds at ATMs. The details of Barkhadle's fraud are as follows.

From December 27, 2017 to February 18, 2018, Barkhadle opened the following fraudulent accounts:

Date	Bank	Name on Account	Account Number	Type of Account
12/27/2017	NASA Credit Union	R.R.	NASA 47609	Credit Card
1/5/2018	Bank of America	Tim Thomas	BOA account 9131	Checking
1/6/2018	Bank of America	Riverfront Construction (Tim Thomas)	BOA account 6384	Business Checking
1/6/2018	Bank of America	Riverfront Construction (Tim Thomas)	BOA account 9367	Business Checking
1/14/2018	Bank of America	R.R.	BOA account 0343	Checking
1/21/2018	Digital Credit Union	R.R.	Digital account 5545	Savings
1/21/2018	Digital Credit Union	R.R.	Digital account 4167	Checking
2/14/2018	Bank of America	Tim Thomas	BOA account 5417	Checking
2/14/2018	Bank of America	Tim Thomas	BOA account 9005	Checking

To open the accounts and obtain loans in the name of R.R., who is a real person, Barkhadle used various means of identification, including R.R.'s name, date of birth, and Social Security number, as well as a fraudulent Wisconsin driver's license in R.R.'s name and bearing his date of birth. A picture of the fraudulent Wisconsin driver's license in R.R.'s name, as well as a pay stub in R.R.'s name, were later found on Barkhadle's phone.

Riverfront Construction was a fictitious business entity created by Barkhadle. Tim Thomas was a fictitious identity created by Barkhadle. To open these accounts, Barkhadle used a false (unassigned) social security number. Mail addressed to Riverfront Construction and Tim Thomas was found during a search of Barkhadle's residence and information about Riverfront Construction, Tim Thomas, and the bank accounts opened in these identities was also located on Barkhadle's phone.

In particular, on January 13, 2018, Barkhadle used R.R.'s name, social security number, and date of birth to obtain a $15,000 loan from Citizens Bank. On March 2, 2018, Barkhadle transferred the loan proceeds to a savings account he had opened in R.R.'s name at Digital Credit Union. The same day, Barkhadle transferred the loan proceeds from the Digital Credit Union savings account to the checking account he had opened at Digital Credit Union, also in R.R.'s name. Five days later, on March 7, 2018, Barkhadle initially transferred $25 of the $15,000 loan

from the Digital Credit Union checking account to the account he had opened in R.R.'s name at Bank of America ("BOA"). The same day, Barkhadle used Zelle, a money transfer service, to transfer $40 from the R.R. account at BOA to different account he had opened at BOA in the name of Riverfront Construction (account ending in 6384).

On March 12, 2018, Barkhadle transferred $2,000 from the R.R. checking account at Digital Credit Union to the R.R. account at BOA. This transfer forms the basis of the wire fraud charge set forth in Count One of the Information. The same day, Barkhadle used Zelle to transfer the same $2,000 from the R.R. account at BOA to the Riverfront Construction account at BOA (6384). Barkhadle withdrew the remaining $13,000 of the fraudulent loan proceeds from the R.R. checking account at Digital Credit Union using ATMs throughout the Milwaukee area.

In addition to transferring loan proceeds Barkhadle obtained using R.R.'s name into the Riverfront Construction account at BOA, Barkhadle used the Riverfront Construction account at BOA to receive proceeds of several "business email compromise frauds." A business email compromise fraud occurs when a fraudster spoofs the email address of a vendor for a victim business. Using this spoofed email address, the fraudster, posing as a legitimate vendor, instructs the victim company to send future payments to a new bank account. In reality, the new bank account belongs to the fraudster, not the victim company's legitimate vendor. In this case, proceeds from three business email compromise frauds were transferred into the Riverfront Construction account Barkhadle had opened at BOA (6384).

On March 13, 2018, a company, E.H., received an email purporting to be from legitimate vendor M.V. LLC providing instructions to send future payments to BOA account 6384. E.H. has no business relationship with Riverfront Construction, Tim Thomas, or Barkhadle. During the period from April 2, 2018 to May 8, 2018, E.H. transferred a total of $26,988.42 to BOA account 6384 in response to this email.

On March 30, 2018, victim company, G.S., transferred a total of $77,093.00 to BOA account 6384. G.S. made this transfer in response to an email that appeared to be from its legitimate vendor indicating that the vendor had changed its banking information and that future payments should be sent to BOA account 6384. G.S. has no business relationship with Riverfront Construction, Tim Thomas, or Barkhadle.

On April 6, 2018, victim company, H.C., transferred $546,241.31 intended for a legitimate vendor, to the Riverfront Construction account at BOA (ending in 6384). On April 16, 2018, H.C. transferred an additional $650,333.26 to the Riverfront Construction account at BOA (6384). H.C. made these transfers in response to an email that appeared to be from its legitimate vendor indicating that its vendor had changed its banking information and that future payments should be sent to BOA account 6384. H.C. has no business relationship with Riverfront Construction, Tim Thomas, or Barkhadle.

Between March 13, 2018 and March 30, 2018, Barkhadle made the following three transfers from BOA account 6384:

- $1,200 to BOA account 6397 on March 13, 2018

- $38,500 to BOA account 6397 on March 30, 2018
- $9,000 to BOA account 9005 on March 30, 2018

On March 30, 2018, Barkhadle transferred $8,000 from BOA account 6397 to BOA account 9131. All of these transfers were transfers of fraudulently obtained funds resulting either from the business email compromise fraud described above or from the fraudulently obtained loan in R.R.'s name.

The next day, on March 31, 2018, Barkhadle withdrew cash from BOA account 9131 and BOA account 9005 at ATMs in Chicago. Photographs from those ATMs confirm Barkhadle is the individual withdrawing the funds. These photographs demonstrate Barkhadle's access to these accounts and show him in possession of the fraudulently obtained funds.

On April 2, 2018, Barkhadle transferred $12,000 from BOA account 6384 to BOA account 5417 and $8,000 from BOA account 6397 to BOA account 5417. As a result of his participation in this scheme, Barkhadle fraudulently obtained approximately $75,000.